IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DiVISION

JONATHAN VILLARREAL, *Plaintiff,* vs. JOHN SAENZ; MIGUEL VILLARREAL, JR; and GUNN, LEE & CAVE, P.C., *Defendants.*	§ § § § § § § § § § §	No. 5:20-CV-00571-OLG

PLAINTIFF'S MOTION TO SANCTION PURSUANT TO FED. R. CIV. P. 11

TO THE HONORABLE JUDGE RICHARD B. FARRER:

COMES NOW, Plaintiff, Jonathan Villarreal, *pro se*, respectfully asking the court to impose sanctions on the entire defense. Plaintiff, Jonathan Villarreal will be using the 1st person "I," and "me" going forward in this document. I am speaking as the owner of Zroblack,LLC in this entire document and NOT FOR Zroblack, LLC.

I. INTRODUCTION

"*Perjury is the basest and meanest and most cowardly of crimes. What can it do? Perjury can change the common air that we breathe into the axe of an executioner.*" - Robert Green Ingersoll.

Cowardice cannot even begin to describe the actions of the defense throughout this entire lawsuit. The scent of oozing pus from an infected sore being fed on by maggots in the blistering heat is a kind depiction of the festerous stench steaming from the vile, and duplicitous actions of the defense.

Spoliation of data, conspiracy, perjury, and ethics violations do not even scratch the surface of this uncivil case. The defense continues to delete data I own, further crippling this case, and hiding evidence of the truth. The defense continues to submit sworn affidavits to the court littered with lies to the extent that they can't even follow their own web of stupidity they have weaved. The defense is knowingly extorting me in documents they have filed, and I can no longer take this.

I warned the defense council June 9th, June 25th, and August 9th, of 2021 that I was going to file sanctions for their continued illegal actions of deletion of company records, submission of false statements, tampering of evidence, and for the defense council's contribution to known illicit activity. I provided photos and document evidence of all the aforementioned and sent them to the defense via email. Follow up emails were sent to the defense to ensure the emails were received, and to also to ensure the lies of never seeing or receiving these emails would not stand when these sanctions would be filed. Every email I sent regarding the illicit actions of the defense were acknowledged by the defense responding to me.

II. PERTINENT FACTS

THE EVERNOTE DATA DELETION PART I

The defense hired a forensic examiner to prove that code sent to John Edward Saenz never existed on my company laptop, and could never exist on my company laptop, or on any other device. The hired forensic examiner Steven S. Broderhausen claimed in his Affidavit that he has

"*Over 30 years of experience in software and computer technology, more than half of which included forensic investigations. I am a Certified Computer Science Examiner and hold a Bachelor of Science degree in Computer Science. I also have experience in, and am familiar with, software development and code writing*" *see* **Dkt No.53 at 10** "**Affidavit of Steven S. BroderHausen**"

First, the defense is hiring a forensics examiner to make sure that they do not have to give my company property back. The laptop was purchased with my company money acknowledged by the defense. The laptop is registered to my company Zroblack, LLC, John Edward Saenz received a 10% Apple Business Discount on this laptop and the Apple Care Plan, only given to Apple Business Partners. Now I ask the court these questions:

1. When the laptop needs repair, and the Apple Genius Bar needs to confirm information about the ownership, and the company associated with the laptop, are you allowing John Edward Saenz to act as a representative of my company? Suppose the court says the laptop ownership documents registered with Apple can be changed into John Edward Saenz's personal name, well I don't approve of that, and if that happens without my approval it is theft, but as long as he doesn't need any repair its not theft right? The court just opened the door for bad actors all around The United States, allowing them to steal from their employers, and have the employer assume all responsibility for the illicit actions performed while in possession of a company registered asset.

2. If taking company property, registered to a company, and purchased by a company, is not stealing company property what is? What does the company own?

3. Since the laptop is registered to Zroblack, LLC, When this laptop becomes part of a botnet to spread ransomware all around the world, or is found to be infested with child pornography, who will be responsible when the serial number is

searched by the FBI? It's not registered to John Edward Saenz, it's registered to my company Zroblack, LLC. Let me remind the court that John Edward Saenz is claiming he is letting his 25 year old son and 16 year old daughter use this laptop for their homework and for "family photos." This in itself is a really funny statement considering that John's son didn't even live at home at the time, and had his own computer. Tristan Hunter Saenz, would text me asking me for help to flash cell phones, and his daughter had her own computer as well. In fact, what a funny scene this would be to see a grown adult and a teenage girl waiting for their turn to use Daddy's personal computer as John Edward Saenz has claimed, to do their homework.

4. Let's suppose I am wrong about everything, and John Edward Saenz's children were in fact waiting in line to use my company laptop, it must have been really hard for them to complete any of their assignments when John Edward Saenz was in Finland with the computer they use for their school work, am I right?

5. The idea of my company laptop floating around with Tristan Hunter Saenz and all of his college friends is incredulous. The idea of John Edward Saenz's daughter surfing the web and infecting the computer with malware is sickening. Does the court take responsibility for the illicit activity that is highly likely to happen on that laptop?

6. By refusing to return my company property, does this mean that the defense accepts all responsibility if child pornography, ransomware, and spyware are distributed with this laptop?

   Texas Penal Code § 46.06 makes certain firearm transfers a crime. For example, it is a crime to knowingly loan or give a firearm to a person, knowing such person intends to use it unlawfully or in the commission of a crime.

7. The liability forcefully being put on my company by the defense and the court is abhorrent, stomach twisting, and unfathomable. Who is responsible for a company asset knowingly stolen from a company by a previous employee? The company asset is still registered to the company, and this asset is used to infect the Texas court systems with ransomware, so who is responsible? Who is paying for my increased business insurance premiums?

It is very interesting how the defense has sent a "forensics expert," someone with a Bachelor's Degree in Computer Science to audit and find the work of a Doctoral Student in Computer Science (me) who writes code so unique there are patents pending. Does it seem logical to have an 8th grader check a college student's work for accuracy? The 8th grader, would have no idea what they are looking for and it is evident in this next statement by Steven S. Broderhausen.

THE EVERNOTE DATA DELETION PART 2

I am familiar with and have used Evernote, the application discussed in the Reply and Unsworn Declaration. Evernote offers web-based data storage accessed with an individual user account. When a user uploads data to Evernote, the data is stored online in cloud-based storage. An Evernote user may access uploaded data from a mobile device or laptop by running the Evernote application and logging in to an Evernote Account. The data is not stored on the device on which the Evernote application runs. A user may access uploaded data and copy it to a device, but simply accessing the data through Evernote does not copy the data to the user's device. see **Dkt No.53 at 11** "**Affidavit of Steven S. BroderHausen**"

This is one of the most concerning things I have ever read in my life. If it is true that his forensics expert has had half of his career in a courtroom, this is a public call for all wrongfully accused to file immediate appeals, and file a malpractice lawsuit against Steven S. BroderHausen, and the councils that knowingly continue to hire this danger to society. This is part of evernote's privacy policy that can be found here https://evernote.com/privacy/policy.

Where does Evernote store my information?

When you use Evernote Software on your computing device, such as by using one of our downloadable applications, some of your data will be stored locally on that device.

When you sync your computing device with the Evernote Service, that data will be replicated on servers maintained in the United States. This means that if you store information in or submit data to the Evernote website or Evernote Software and sync such Evernote Software with the Evernote Service, you acknowledge your personal information will be transmitted to, hosted, and accessed in the United States.

Data privacy laws or regulations in your home country may differ from, or be more protective than, those in the United States. We will collect, store, and use your personal information in accordance with this Privacy Policy and applicable laws, wherever it is processed.

Let's pause here for a minute, and reflect, Evernote themselves state that your data will be stored locally if you are using their downloadable applications.

Steven S. BroderHausen continues to state, "Since my prior affidavit, dated February 4th, 2021, I personally re-examined the Computer. None of the six files identified in the Unsworn Declaration at paragraphs 9,10 and 17 are present on the Computer. The computer contains no database files for Evernote. The computer contains no local files for Evernote". see ***Dkt No.53 at 11 "Affidavit of Steven S. BroderHausen"***

THE EVERNOTE DATA DELETION PART 3

Let me remind the court that this statement from the expert witness was one of the reasons that you have denied my injunctive relief, and temporary restraining order. I suppose this may not be enough for the court to reverse its decisions, so let me proceed.

Ah yes, "The Affidavit of John Saenz," a document I like to call the Saenz of Fraud. I'll go back and address all of the lies, but for the purpose of showing the court how deep in this fraud we are in, I am going to stick to these consecutive whoppers of a lie by John Edward Saenz. Enjoy.

"*Upon ZroBlack's receipt of the initial payment of $1.5 million from the Foreign Customer, Zroblack provided both Villarreal and me with a distribution of $740,000 consistent with our equal interest in ZroBlack. The remaining $20,000 remained in ZroBlack's account for operating capital (though, at the time, ZroBlack had no employees or rent and very little overhead or expenses)"* ***Dkt No.42 at 14 "The Affidavit of John Saenz"***

"*Since the Computer was purchased, I have used it for my own personal use with Villarreal's knowledge. To my knowledge, Villarreal has never possessed or used the Computer for Zroblack's business or otherwise. Among other files, the Computer contains my family photos, my resume, and even my children's homework. As Such, at all relevant times, the Computer has been treated as my personal laptop rather than ZroBlack's property." see* ***Dkt No.42 at 15 "The Affidavit of John Saenz"***

1. John Edward Saenz admits that $20,000 was left in ZroBlack's bank account and was to be used for operating capital. Exhibit 5, shows John Edward Saenz purchasing a company laptop from Apple, with AppleCare, registering the computer in Zroblack's name, and even associating the computer purchased to a Zroblack email address which he used, je@zroblack.com Not pictured is the 10% discount that was given to Zroblack for being part of the Apple Business Team. Exhibit 5 shows the deduction of funds coming from Zroblack's business bank account that had $20,000 of operating capital in it.

2. If we follow the "Saenz of Fraud," John Edward Saenz specifically states that this computer paid for with company funds, intended for the operations of the company has at "*all relevant times, the Computer has been treated as my personal laptop rather than ZroBlack's property."*

3. Ok, this is getting weird, John Edward Saenz is literally admitting to stealing my company money and depriving me of my company assets and funds, instantly making me liable for all of his actions performed with that laptop because he had the clear intent of never using it as ZroBlack's property.

4. So you have already taken $740,000, you decide to suck the company dry with a "personal" laptop? If I would have known John was going to use this laptop as a personal laptop, I would have said, what's wrong with you these are company funds, we need this money to help grow our business. This literally makes no sense, why leave $10,000's each into the business bank account if you're just going to start sucking it dry with your own personal items?

5. I think I do have to remind everyone that this notion that you can use company funds for personal items with no consequence comes from the person that says, "*I then worked as an independent financial advisor until 2018 when I sold my practice and had the opportunity to form Zroblack, LLC, Prior to my time with ZroBlack, my business experience included finances and marketing, as well as more than 20 years of face-to face business and client counseling and negotiations" **Dkt No.42 at 15** "**The Affidavit of John Saenz**"*

6. This pro with more than 20 years of business experience is blatantly stealing from the company? No, I cannot believe this, it has to be some sort of mix up? Shamefully, it's not.

We have established that John Edward Saenz was defrauding the company, by his own words in an affidavit that can carry criminal charges if proven to be false, now let's get to the meat of the fraud.

I filed **Exhibit 43**, a picture of John Edward Saenz, and this "personal use" macbook pro in Tampere, Finland. I filed Exhibit 44, and zoomed in on the image of the MacOS dock. The court or the defense didn't care about this, but maybe it's because we can't speak to each other like we're humans and we have to legally vomit all over something that is so simple.

Exhibit 44 shows a bunch of icons at the bottom of a Macbook Pro that my company owns. John has claimed that this is his "personal computer", and has never conducted business on it but yet it is with him in Tampere, Finland, on our business trip. When you look at the icons in the bottom of the Macbook Pro, right next to the Google Chrome icon is a terminal icon, and it's open, how do I know it's open? The applications that are open all have a white dot under them. Why is this important? Why does John have a terminal application on his personal computer?

"Given that my background is purely in business and finance, I have no training, or experience in writing or interpreting computer code. I have never formally or informally studied computer programming, do not know how to write computer code or otherwise use programming software, and I have never interpreted code and do not understand how the code writing or interpreting process works. I have have never taken any coding classes" ***Dkt No.42 at 15 "The Affidavit of John Saenz"***

Here are some more questions for the court:

1. What was John doing in Finland on that work trip with his personal laptop?

2. John says, "Villareal and I created ZroBlack for the purpose of marketing and monetizing certain technologies developed by Villareal" How could John market and monetize the technology I built if he didn't know how it ran, didn't have a copy of the software, and had no intellectual property documents at all regarding this technology?

3. How could John have closed this deal?

On May 9th, 2019 John Edward Saenz sent an email to the VP of R&D for Zroblack's foreign client.

"Daniel, Please email me the login information so that I may copy my logs. As I mentioned yesterday, I started the logs when I first arrived. I wanted both ZroBlack and Blancco to have a record of all the progress we were making. This is also an added benefit for accounting, auditing, and tracking purposes. I will copy my logs every morning for the previous day" Exhibit AA

1. Hold on, wait a minute, how is he sending these emails while we are in Finland, and he only has his personal laptop with him?

2. Why is the Zroblack email disclaimer at the bottom of the….oh, I see, because John was sending emails from the ZroBlack email account that I helped him set up on Mac Mail. You can see Mac Mail open in Exhibit 44.

3. What a minute, how is it that John is going to copy his logs every morning to the foreign client's project management portal if he only has his personal laptop?

Finally, after all the stupid lies, and deception about never having any proprietary code or there being any spot of Evernote ever being on John's "personal" laptop that contained proprietary code or intellectual property, we come to a full stop on this entire bullshit lie.

THE EVERNOTE DATA DELETION PART 4

The great thing about Evernote is that the logging and tracking is so beneficial to a coder like myself. The geo location tagging of every note, metadata grabs and so much more are what actually helped me secure this contract with the foreign client. I could prove that I wrote this code on my own time, at my house, and anyone that would try to contest these facts would be stopped in their tracks because Evernote takes multiple log syncs of the notes you take. Their icon is an elephant as in an elephant never forgets.

You're probably thinking, Jonathan what's the point, TLDR, and I would absolutely agree, but the mounds of hot shit this case is littered with takes time to sift through and explain to everyone because this is part of the fraud, misdirection.

Let me do a short, Evernote Data Deletion Round Up. What did we learn?

1. John used company funds to purchase a "personal" computer from the Apple store, with the intent to defraud Zroblack, because what other reason would you have to use company money for your own personal gain, while depriving the company of what is rightfully theirs?

2. John lied about the computer only being used as a "personal" computer, because we caught him in another lie via an Email to the VP of R&D.

3. Steven Broderhausen is dangerous and should be stripped of his license and authority to act as an expert witness.

4. Steven Broderhausen continuously fed this court and this case false information that impacted the decision of the case to favor the defendants.

5. Evernote does store data on your machines, and it is written in their privacy policy.

Ok, we are all caught up so far, and now for the big reveal. The following exhibit was given to the defense June 25th, 2021, more than a month before Chief Judge Orlando L. Garcia signed the order adopting Judge Richard B. Farrer's recommendations. Exhibit U, is an email I sent to David Vanderhider, and Ryan Sullivan.

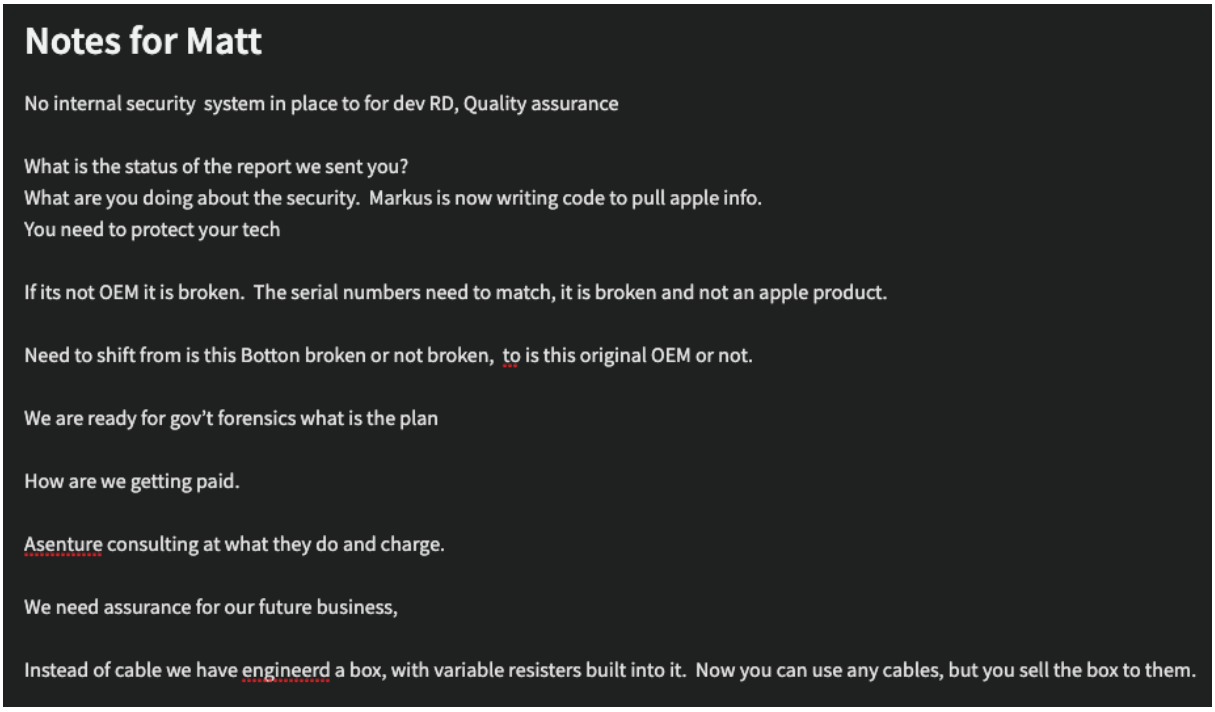
This email included factual and alerting discoveries that alter this case as it stands.

1. The lies of John never having any proprietary information or code on the company computer show its face, the lies of never having any knowledge of or noticing any Evernote application was ever on his computer fails on its face.

2. I provide the defense screenshots of the meta data taken from Evernote documents written by John Edward Saenz himself using je@zroblack.com as the Evernote Login. It should start to make sense now to the court, that one of the reasons John has refused to turn over the email server, and deleted my data on the email server is because Evernote is amazing at logging, and sending email notifications when you have been sent a document to and from someone.

3. More profoundly is the context of one of the Evernote documents that John wrote and shared with me, and is the large subject of the denied motion for injunctive relief and temporary restraining order, fraud, and more.

4. John specifically states the following in a note he was preparing to send to the CEO of our foreign client.



Notes for Matt

No internal security system in place to for dev RD, Quality assurance

What is the status of the report we sent you?
What are you doing about the security. Markus is now writing code to pull apple info.
You need to protect your tech

If its not OEM it is broken. The serial numbers need to match, it is broken and not an apple product.

Need to shift from is this Botton broken or not broken, to is this original OEM or not.

We are ready for gov't forensics what is the plan

How are we getting paid.

Asenture consulting at what they do and charge.

We need assurance for our future business,

Instead of cable we have engineerd a box, with variable resisters built into it. Now you can use any cables, but you sell the box to them.

"What are you doing about security, Markus is now writing code to pull Apple info, you need to protect your code, we are ready for government forensics what's the plan" **Exhibit U-E**

5. All of this wasted time, lies, deceit, and forensic idiocy was for what?
6. The meta data I provided to the defense council is clear. I have exported the evernote document in html form so the source code can be read, and it includes the following. **Exhibit U-F**

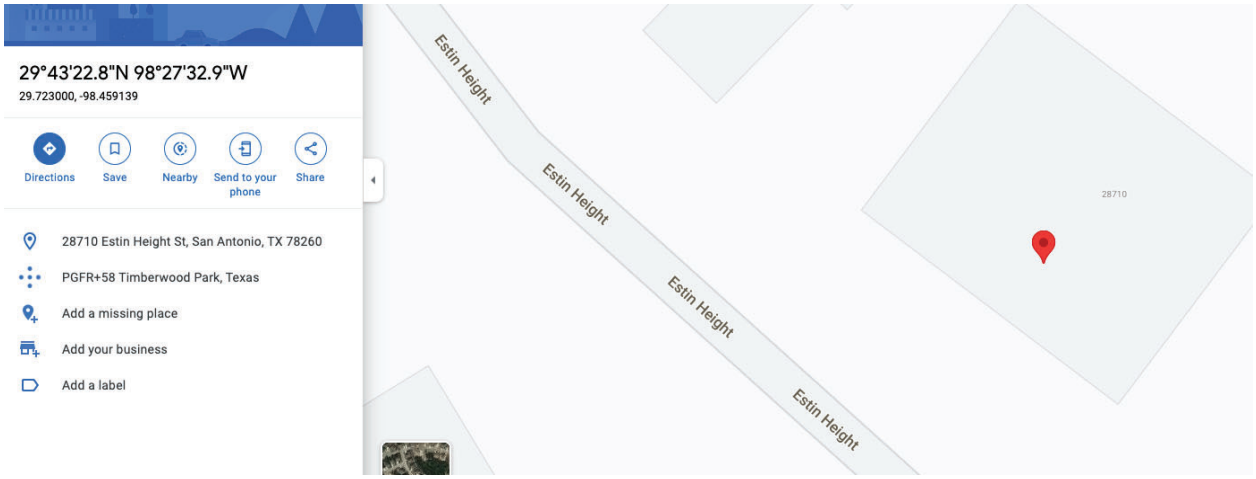
    a. The author is John Saenz **Exhibit U-G**
    b. The author's email address is je@zroblack.com **Exhibit U-G**
    c. The date it was created was Thursday May 23rd, 2019 @11:16am
    d. The last day it was updated was Monday May 27th, 2019 @ 2:20pm
    e. The computer used to create this note and application was the macbook pro this lawsuit is over among other things

f. The lat, long of where the note was taken takes you directly to

i. Exhibit-U-H

ii. John's house, it is an exact dead on pinpoint

1. Lat: 29.723007202148438
2. Long: -98.45912943999996



7. These are not the only notes that John sent me from je@zroblack.com

   a. John was an active evernote user on his mobile device, macbook pro purchased by the company, and evernote web clipper for chrome. All the metadata live in multiple copies on the Evernote servers and it is irrefutable evidence.

8. John knew how sensitive information this was, and he knew that my inventions would become matters of national security if they were removed from our company space. John's failed attempt to cover up these lies and the defense council's active roll in this conspiracy warrants disbarment, and a transfer to the district attorney's office for criminal prosecution.

ACTIVE SPOLIATION OF DATA

_____As if things couldn't get any worse, John Saenz is further trying to cover his tracks from the lies and fraud he has created around him. In the same email I sent to the defense council, I exclaimed that John had deleted my company LinkedIn page, a business portal that had many important and sensitive conversations in the inbox including a conversation with Kevin Mitnick, Our foreign client leaders, and personal friends of mine in the security industry I had introduced John to.

John had been using Zroblack's LinkedIn for over a year and a half after the release was signed, and then as the irons were getting hot, he deleted the account all together. Again the defense council was 100% aware of this, and did nothing to alter the court, and continued to conceal the fraud. **Exhibit U**

Exhibit 39 Page 8 Clearly defines http://linkedin.com/in/john-e-saenz-zroblack as an asset of my company Zroblack. Impersonating a manager or director of Zroblack for more than a year is the lowest of low, and deleting the business messages along with the entire account is criminal. Exhibits **U-B, U-C, U-D**, show John actively using the Zroblack linkedIn account in early June 2021, and then deleting the account entirely when I email the defense council June 25th, 2021

PRAYER FOR RELIEF

The facts of this conspiracy, and fraud need to be revealed, the release was signed under 100% duress, there were 3 releases signed, and I begged Mike Villarreal to release me 5 times as a client, but he refused. The defense is still extorting me for $85,000, and if what I have just provided to the court is not proof enough that I am telling the truth in all of this, then I am out of options! I have the proof for everything I am claiming, and this is all part of a larger conspiracy. I am officially whistleblowing on the fraud that involves John Saenz, and Former Army Pentagon Col. Dawn Devine, and their attempt to defraud the US Government out of over $300M USD in government contracts using my technology. I refused to be party to their fraud, and scams, and I refused to give Col. Devine an executive seat in my company Zroblack, LLC. As she was

actively working in the Pentagon, John and Col. Devine devised a plan to defraud the US Government by John claiming Zroblack was a disadvantaged company, and Col. Devine writing Zroblack's capabilities paper. Col. Dawn Devine coached John on how to win this contract with USSOCOM, and Col. Devine said that winning was no issue. I was told by John that the Col. knows I created a single source solution, eliminating any competition. I had many encrypted video chats, and I even have emails forwarded from Col. Devine's .mil email address with Army Contracts NOT available to the public. There is no wonder why I have been denied access to the Zroblack government logins, I hope the court can start to put all the pieces together.

I am tired of this bullshit, and I want justice. I want the criminals put in jail so that they can never do this to anyone ever again. I want to believe in the US justice and court system again. I am a proud American, and this is disgraceful to all of us.

Respectfully, Submitted,

Jonathan Villarreal, Plaintiff, *pro se*

jonathan villarreal

28251 Boerne Stage Rd

Boerne, TX 78006

830-499-3071

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was electronically filed with the Court on the 21st day of September 2021, and electronically served on the date reflected in the ECF system upon all parties registered to receive notice pursuant to the Court's CM/ECF system.

jonathan villarreal

Jonathan Villarreal, *pro se*